DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JAN 0 8 2001

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Destruction of DoD Computer Hard Drives Prior to Disposal

Historically, the Department's policies regarding sanitization and destruction of computer hard drives have been applied only to equipment that processed classified information. More recently, the proliferation of networked unclassified desktop computers, with their ability to retain vast amounts of information, and the resultant possibility of increased sensitivity of the aggregated data, dictated that we properly sanitize unclassified computer equipment before it is turned in for disposal or reutilization. Notwithstanding these precautions, preliminary results of a recent Inspector General audit have revealed instances of sensitive information remaining on computer hard drives that had been certified as having been "wiped" clean (i.e., they contain no sensitive information) prior to disposal or reutilization outside DoD.

Accordingly, I direct that you take immediate steps to ensure that all hard drives of unclassified computer equipment being disposed of outside DoD are removed and destroyed. Guidance for destruction may be found at ***http://www.c3i.osd.mil/org/sio/ia/diap/***.

The Assistant Secretary of Defense (C3I) will assess this implementation and determine, within 12 months, if further adjustments are warranted. Questions concerning this memorandum may be directed to Mr. Donald Jones, OASD(C3I)/IA, at 703-614-6640.

Rudy de Leon

U16448 /00

Guidance for Destruction of DoD Computer Hard Drives (Unclassified) Prior to Disposal

1. Deputy Secretary of Defense memorandum, Subject: "Destruction of DoD Computer Hard Drives Prior to Disposal," dated January 8, 2001 (Enclosure 1) directs all DoD Components to "take immediate steps to ensure that all hard drives of **unclassified** computer equipment being disposed of outside DoD are removed and destroyed." The intent of this memorandum is to prevent DoD Sensitive information, as defined in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, from being obtained from computers being disposed of by DoD.

2. The term "hard drive" as used in the memorandum includes:

a) Rigid magnetic storage media such as removable disk packs; (e.g., single and multiple platter disk packs); sealed disk drives, hard disk assemblies (HDAs); and magnetic Bernoulli cartridges.

b) Optical storage media such as optical disks, optical tape, and optical Bernoulli cartridges.

3. Acceptable means to destroy rigid magnetic media are described below. Further, system administrators are highly encouraged to perform overwrite or 'wipe disk' procedures on functioning disk drives before CPUs are turned in for disposal by using a pseudo-random overwrite utility that is available with such products as Norton Utilities and similar products. This will decrease accessibility to the data until such time as the formal destruction procedures are implemented.

a) Sanitization by bulk degaussing: Remove the hard drive from the chassis or cabinet. Remove any steel shielding materials or mounting brackets, which may interfere with the magnetic fields. Place the hard disk drive in an approved NSA/CSS approved degausser (National Security Agency Degausser Products List) and erase at the required field setting. The bulk erasure of sealed disk packs or hard drives will cause damage (i.e., loss of timing tracks and damage to disk drive motor) which will prohibit its continued use. However, if there is any doubt that the degaussing was not successful, further physical disabling in paragraph b) below should be conducted. Specific questions regarding NSA approved products/procedures should be directed to NSA's INFOSEC Service Center at 1-800-688-6115 or DSN 238-4399.
(Note: Degaussing should only be conducted by personnel with technical knowledge about the equipment who routinely conduct these procedures for the degaussing of **classified** disks.)

b) Physical destruction/impairment beyond reasonable use: Remove the hard drive from the chassis or cabinet. Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit. The hard drive should then be subjected, in a suitable facility with individuals wearing appropriate safety equipment, to physical force or extreme temperatures (e.g., pounding with a sledge

hammer; incinerator) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be re-inserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be re-connected without significant rework.

4. Optical mass storage media, including compact disks (CD, CDE, CDR, CDROM), optical disks (DVD), and magneto-optic disks (MO) must be destroyed by burning, pulverizing, or grinding the information bearing surface. When material is pulverized or ground, all residue must be reduced to pieces sized 0.25 millimeter or smaller. Burning shall be performed only in a facility certified for the destruction of classified materials.

5. As a reminder, paragraph 6-701 of DoD Regulation 5200.1-R, "DoD Information Security Program," dated January 1997, directs Components to obtain guidance on appropriate methods for destroying **classified** electronic media and equipment from NSA. The instructions regarding destroying unclassified media provided above are largely based on NSA procedures for the sanitization or destruction of classified media.